Network Working Group T. Socolofsky
Request for Comments: 1180 C. Kale
Spider Systems Limited
Enero 1991

Un Tutorial de TCP/IP

Estado de la memoria

Este RFC es un tutorial del conjunto TCP/IP, centrándose en particular en los pasos que sigue un datagrama IP desde el host fuente hasta el host destino a través de un router. No especifica un estándar de Internet. Se permite la distribución ilimitada de esta memoria.

Indice de Contenidos

1. Introducción..... 1
2. Perspectiva general TCP/IP 2
3. Ethernet..... 8
4. ARP..... 9
5. Protocolo Internet (IP)..... 12
6. Protocolo de datagrama de usuario (UDP)..... 22
7. Protocolo de Control de la Transmisión (TCP)..... 24
8. Aplicaciones de red..... 25
9. Otra información..... 27
10. Referencias..... 27
11. Relación con otros RFCs..... 27
12. Consideraciones de seguridad..... 27
13. Direcciones de los autores..... 28

1. Introducción

Este tutorial sólo contiene una visión de los puntos más llamativos de TCP/IP, así como los fundamentos de la tecnología TCP/IP. Se omite la historia del desarrollo y fundación, el asunto de su uso y su futuro comparado con OSI de ISO. En efecto, mucha información técnica también se omite. Lo que queda es un mínimo de información que debería ser entendida por profesionales del entorno TCP/IP. Estos profesionales incluyen al administrador del sistema, al programador del sistema y al administrador de la red.

Este tutorial usa ejemplos del entorno TCP/IP UNIX, no obstante los puntos principales son aplicables a todas las implementaciones de TCP/IP.

Nótese que el propósito de esta memoria es la explicación, no la

definición. Si surge cualquier cuestión acerca de la correcta especificación del protocolo, por favor remítase al estándar de definición RFC actual.

La próxima sección es una ojeada a TCP/IP, seguida de descripciones detalladas de componentes individuales.

2. Perspectiva general TCP/IP

El término genérico "TCP/IP" usualmente significa cualquier cosa y todo con referencia a los protocolos específicos TCP e IP. Pueden incluir otros protocolos, aplicaciones e incluso los medios de red. Un ejemplo de estos protocolos son: UDP, ARP e ICMP. Un ejemplo de estas aplicaciones son: TELNET, FTP y RPC. Un término más preciso es "tecnología internet". A una red que usa una tecnología internet se le llama una "internet".

2.1 Estructura básica

Para entender esta tecnología primero debe entender la siguiente estructura lógica:

```
                      ----------------------------
                      |    aplicaciones de red   |
                      |                          |
                      |...   | /  ..   | /  ...|
                      |     -----      -----     |
                      |     |TCP|      |UDP|     |
                      |     -----      -----     |
                      |               /         |
                      |         --------         |
                      |         |  IP  |         |
                      |  -----  -*------         |
                      |  |ARP|   |              |
                      |  -----   |              |
                      |         |              |
                      |      ------             |
                      |      |ENET|             |
                      |      ---@--             |
                      ----------|-----------------
                                |
          ----------------------o---------
              Cable Ethernet
```

Figura 1. Nodo de red básico TCP/IP

Esta es la estructura lógica de los protocolos divididos en capas dentro de un computador en una internet. Cada computador que se puede comunicar usando una tecnología internet tiene también una estructura

lógica. Es esta estructura lógica la que determina el comportamiento del computador en la internet. Las cajas representan el procesado de los datos conforme van atravesando el computador y las líneas que conectan las cajas muestran el camino de los datos. La línea horizontal de abajo representa el cable de Ethernet, el "o" es el transceptor. El "*" es la dirección IP y la "@" es la dirección Ethernet. Entender esta estructura lógica es esencial para entender la tecnología internet; hay referencias a ella a lo largo de todo este tutorial.

2.2 Terminología

El nombre de una unidad de datos que fluye a través de una internet depende de donde se encuentre en la pila de protocolos. En resumen: si está en una Ethernet se le llama trama Ethernet; si está entre el driver Ethernet y el módulo IP se le llama un paquete IP; si está entre el módulo IP y el módulo UDP se le llama datagrama UDP; si está entre el módulo IP y el módulo TCP se le llama segmento TCP (o más generalmente un mensaje de transporte); y si está en una aplicación

de red se le llama mensaje de aplicación.

Estas definiciones son imperfectas. Las definiciones actuales varían de una publicación a otra. Unas definiciones más específicas pueden encontrarse en: http://www.faqs.org/rfcs/rfc1122.html (RFC1122) sección 1.3.3.

Un driver es un software que comunica directamente el interfaz hardware de red. Un módulo es un software que comunica con un driver, con aplicaciones de red o con otro módulo.

Los términos driver, módulo, trama Ethernet, paquete IP, datagrama UDP, mensaje TCP y mensaje de aplicación se usan apropiadamente a lo largo de este tutorial.

2.3 Flujo de datos

Sigamos los datos tal como fluyen hacia abajo a lo largo de la pila de protocolos mostrada en la Figura 1. Para una aplicación que usa TCP (Transmission Control Protocol - Protocolo de Control de Transmisión), los datos pasan entre la aplicación y el módulo TCP. Para aplicaciones que usan UDP (User Datagram Protocol - Protocolo de Datagrama de Usuario), los datos pasan entre la aplicación y el módulo UDP. FTP (File Transfer Protocol - Protocolo de Transferencia de Ficheros) es una aplicación típica que usa TCP. En este ejemplo su pila de protocolos es FTP/TCP/IP/ENET. SNMP (Simple Network Management Protocol - Protocolo Simple de Control de la Red) es una aplicación que usa UDP. En este ejemplo su pila de protocolos es SNMP/UDP/IP/ENET.

El módulo TCP, el módulo UDP y el driver Ethernet son multiplexores n-a-1. Como multiplexores conmutan muchas entradas hacia una sola salida. También son demultiplexores 1-a-n. Como demultiplexores conmutan una entrada hacia muchas salidas, de acuerdo al campo de tipo en la cabecera del protocolo.

```
1   2 3 ...   n                  1   2 3 ...   n
   |      /      |                | |      /       ^
   | |   /       |                | |     /        |
-------------   flujo            ----------------   flujo
|multiplexor|    de              |de-multiplexor|    de
-------------   datos            ----------------   datos
     |            |                    |              |
     |            v                    |              |
     1                                 1
```

Figura 2. multiplexor n-a-1 y demultiplexor 1-a-n

Si una trama Ethernet sale desde el driver de Ethernet hacia la red, el paquete puede pasar por el módulo ARP (Address Resolution Protocol - Protocolo de Resolución de Direcciones) o por el módulo IP. El valor del campo de tipo en la trama Ethernet determina por dónde pasa la trama Ethernet, por el módulo ARP o por el módulo IP.

Si un paquete IP sube a través del módulo IP, la unidad de datos pasa al módulo TCP o al UDP, lo cual viene determinado por el valor del campo de protocolo en la cabecera IP.

Si el datagrama UDP sube a través del módulo UDP, el mensaje de aplicación pasa a la aplicación de red basándose en el valor del campo de puerto de la cabecera UDP. Si el mensaje TCP sube a través

del módulo TCP, el mensaje de aplicación pasa a la aplicación de red basándose en el valor del campo del campo de puerto en la cabecera TCP.

La multiplexación hacia abajo es simple de ejecutar, ya que para cada punto de partida sólo hay un camino hacia abajo; cada módulo de protocolo añade su información de cabecera para que el paquete pueda ser demultiplexado en el computador destino.

Los datos que pasan desde las aplicaciones a través de TCP o de UDP convergen en el módulo IP y se envían hacia abajo a través del driver de interfase de red.

Aunque la tecnología internet soporta muchos y diferentes medios de red, en este tutorial se usa Ethernet para todos los ejemplos, ya que es la red física bajo IP más común. El computador de la Figura1 tiene

una conexión Ethernet simple. La dirección Ethernet de 6 bytes es única para cada interfase en una Ethernet y está localizada en el interfase más bajo del driver de Ethernet.

El computador también tiene una dirección IP de 4 bytes. Esta dirección está localizada en el interfase más bajo del módulo IP. La dirección IP debe ser única en una internet.

Un computador en funcionamiento conoce siempre su propia dirección IP y Ethernet.

2.4 Dos interfaces de red

Si un computador está conectado a dos Ethernet separadas, como se muestra en la Figura 3

```
                 ----------------------------
                 |    aplicaciones de red   |
                 |                          |
                 |...   | /  ..   | /  ...|
                 |     -----      -----     |
                 |     |TCP|      |UDP|     |
                 |     -----      -----     |
                 |               /         |
                 |         --------         |
                 |         |  IP  |         |
                 |  -----  -*----*-  -----  |
                 |  |ARP|   |    |   |ARP|  |
                 |  -----   |    |   -----  |
                 |         |    |   /      |
                 |      ------  ------      |
                 |      |ENET|  |ENET|      |
                 |      ---@--  ---@--      |
                 ----------|-------|---------
                           |       |
                           |    ---o----------------------------
                           |             Cable Ethernet 2
             ---------------o----------
               Cable Ethernet 1
```

Figura 3. Nodo de red TCP/IP en 2 Ethernet

Fíjese en que este computador tiene dos direcciones Ethernet y dos direcciones IP.

De esta estructura se ve que para computadores con más de una interfase física de red, el módulo IP es tanto un multiplexor n-a-m como un demultiplexor m-a-n


```
1   2 3 ...   n                  1   2 3 ...   n
   | |      /    |                | |      /       ^
   | |     /     |                | |     /        |
-------------   flujo            ----------------   flujo
|multiplexor|    de              |de-multiplexor|    de
-------------   datos            ----------------   datos
  / | |          |                / | |             |
 /  | |          v               /  | |             |
1   2 3 ...   m                  1   2 3 ...   m
```

Figura 4. multiplexor n-a-m y de-multiplexor m-a-n

Se lleva a cabo esta multiplexación en ambas direcciones para dar cabida a los datos de entrada y de salida. Un módulo IP con más de un interfase de red es más complejo que nuestro ejemplo original en el cual se pueden enviar datos hacia delante sobre la red próxima. Los datos pueden llegar a cualquier interfase y ser enviados a cualquier otro.

```
                         TCP      UDP
                                 /
                                /
                       --------------
                       |     IP     |
                       |            |
                       |    ---     |
                       |   /       |
                       |  /     v   |
                       --------------
                        /                                  /
                  los datos     los datos
                      entran por    salen por
                      aquí          aquí
```

Figura 5. Ejemplo de reenviado de un paquete IP

El proceso de enviar un paquete IP sobre otra red se llama enrutamiento o reenvío de un paquete IP. Un computador que ha sido dedicado a la tarea de enrutar o reenviar paquetes IP se llama un "router o enrutador IP".

Como puede observar en la figura, el paquete IP enrutado nunca llega al módulo TCP y UDP del router IP. Algunas implementaciones de routers IP no tienen módulos TCP o UDP.

2.5 IP crea una red lógica individual

El módulo IP es básico para el éxito de la tecnología internet. Cada módulo o driver añade su cabecera a los mensajes y los mensajes

atraviesan hacia abajo la pila de protocolos. Cada módulo o driver elimina la cabecera correspondiente del mensaje conforme éste sube por la pila de protocolos hacia la aplicación. La cabecera IP contiene la dirección IP, la cual construye una red lógica individual a partir de múltiples redes físicas. Esta interconexión de redes físicas es el origen del nombre: internet. Una serie de redes físicas interconectadas que limitan el rango de un paquete IP se llama una "internet".

2.6 Independencia de la red física

IP esconde a las aplicaciones de red el hardware de red que está en la base. Si usted inventa una nueva red física, puede ponerla en funcionamiento implementando un nuevo driver que conecte a internet bajo IP. De esta forma, las aplicaciones de red permanecen intactas y no se ven afectadas por los cambios en la tecnología hardware.

2.7 Interoperabilidad

Si dos computadores en una internet puede comunicarse, ello se llama "interoperar"; si una implementación de la tecnología internet es buena, se dice que tiene "interoperabilidad". Los usuarios de computadores de propósito general se benefician de la instalación de una internet debido a la interoperabilidad de los computadores en el mercado. Generalmente, cuando usted compra un computador, éste interoperará. Si el computador no tiene interoperabilidad y la interoperabilidad no puede ser añadida, éste ocupa un lugar extraño y especial en el mercado.

2.8 Tras el primer vistazo

Con los conocimientos de base, contestaremos a las siguientes preguntas:

Cuando se envía un paquete IP, ¿cómo se determina la dirección Ethernet?

¿Cómo sabe IP cuál de los múltiples interfaces de red debe usar al enviar un paquete IP?

¿Cómo un cliente en un computador alcanza el servidor en otro computador?

¿Por qué existe TCP y UDP en lugar de existir o uno o el otro?

¿Qué aplicaciones de red están disponibles?

Esto será explicado, por partes, tras un recordatorio de Ethernet.

3. Ethernet

Esta sección es un corto recordatorio de la tecnología Ethernet.

Una trama Ethernet contiene la dirección destino, la dirección origen, el campo de tipo y los datos.

Una dirección Ethernet es de 6 bytes. Cada dispositivo tiene su propia dirección Ethernet y escucha para recibir tramas con esta dirección de destino. Todos los dispositivos también escuchan para recibir tramas con una dirección destino comodín de "FF-FF-FF-FF-FF-FF" (en hexadecimal), llamada una dirección de difusión ("broadcast").

Ethernet usa CSMA/CD (Carrier Sense and Multiple Access with Collision Detection - Acceso Múltiple y Detección de Portadora con Detección de colisiones). CSMA/CD significa que todos los dispositivos se comunican en un medio simple, que sólo uno de ellos puede transmitir a la vez, y que todos ellos pueden recibir a la vez. Si dos dispositivos intentan transmitir en el mismo instante, la colisión de la transmisión se detecta y ambos dispositivos esperan durante un tiempo aleatorio (pero corto) antes de intentar transmitir de nuevo.

3.1 Una analogía humana

Una buena analogía de la tecnología Ethernet es un grupo de personas hablando en una pequeña habitación completamente a oscuras. En esta analogía, el medio físico de red son las ondas sonoras en el aire en lugar de las señales eléctricas en un cable coaxial.

Cada persona puede oír las palabras cuando otra está hablando (Detección de Portadora). Todo el mundo en la habitación tiene capacidad para hablar (Acceso Múltiple), pero ninguno de ellos habla durante mucho tiempo porque son educados. Si una persona es maleducada, se le pide que deje la habitación (por ejemplo, echarla de la red).

Nadie habla mientras otra persona está hablando. Pero si dos personas empiezan a hablar en el mismo instante, cada uno de ellas sabe que esto ha sucedido debido a que han escuchado algo que ellas no han dicho (Detección de Colisión). Cuando estas dos personas se dan cuenta de esta situación esperan un momento, después una de ellas empieza a hablar. El otro escucha lo que se dice y espera a que la primera persona termine de hablar antes de empezar a hablar ella misma.

Cada persona tiene un nombre único (una dirección Ethernet única) para evitar confusiones. Cada vez que una de ellas habla, empieza el mensaje con el nombre de la persona con quien está hablando y con su propio nombre (dirección Ethernet destino y origen, respectivamente) por ejemplo, "Hola, Jane, soy Jack, ...blah, blah, blah...". Si quien habla quiere hacerlo a todo el mundo debe decir "a todo el mundo" (dirección de difusión), por ejemplo, "Hola a todo el mundo, soy Jack,
...blah, blah, blah...".

4. ARP

Cuando se envía un paquete IP, ¿cómo se determina la dirección Ethernet destino?

ARP (Address Resolution Protocol - Protocolo de Resolución de Direcciones) se usa para traducir direcciones IP a direcciones Ethernet. La traducción se hace sólo para paquetes salientes, ya que es cuando se crean la cabecera IP y la cabecera Ethernet.

4.1 Tabla ARP para traducción de direcciones

La traducción se lleva a cabo buscando el una tabla. La tabla, llamada tabla ARP, se guarda en memoria y contiene una fila por cada computador. Hay una columna para la dirección IP y una columna para la dirección Ethernet. Cuando se traduce una dirección IP a una dirección Ethernet, se busca en en la tabla la dirección IP correspondiente. La siguiente es una tabla ARP simplificada:

dirección IP	dirección Ethernet
223.1.2.1	08-00-39-00-2F-C3
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

TABLA 1. Ejemplo de tabla ARP

El convenio para escribir los 4 bytes de la dirección IP es escribir cada byte en decimal y separar los bytes con un punto. Cuando se escriben los 6 bytes de la dirección Ethernet, el convenio es cada byte en hexadecimal y separar los bytes con un guión o con dos puntos.

La tabla ARP es necesaria, ya que la dirección IP y la dirección Ethernet se escogen de forma independiente, no puede usar un algoritmo para traducir direcciones IP a direcciones Ethernet. La

dirección IP se escoge por el administrador de red, basándose en la localización del computador en la internet. Cuando el computador se mueve a una parte diferente de la internet, su dirección IP debe ser cambiada. La dirección Ethernet es seleccionada por el fabricante de la tarjeta de red, basándose en las direcciones Ethernet reservadas para el fabricante. Cuando la tarjeta interfase de hardware Ethernet cambia, la dirección Ethernet cambia.

4.2 Escenario típico de traducción

Durante un funcionamiento normal, una aplicación de red, como TELNET, envía un mensaje de aplicación a TCP, después TCP envía el correspondiente mensaje TCP al módulo IP. La dirección IP destino es conocida por la aplicación, el módulo TCP, el módulo IP. En este punto, el paquete IP ha sido construido y está listo para enviarse al driver Ethernet, pero primero se debe determinar la dirección Ethernet.

La tabla ARP se usa para buscar la dirección Ethernet destino.

4.3 La pareja Petición/Respuesta ARP

Pero, ¿Cómo se rellena la tabla ARP en primer lugar? La respuesta es que se rellena automáticamente por ARP basándose en las necesidades. Dos cosas ocurren cuando la tabla ARP no puede ser usada para traducir una dirección:

1. Un paquete de petición ARP con una dirección Ethernet de broadcast se envía a la red a cada computador.

2. El paquete IP saliente se pone en una cola.

Cada interfase Ethernet de cada computador recibe el broadcast de la trama Ethernet. Cada driver Ethernet examina el campo de tipo en la trama y pasa el paquete ARP al módulo ARP. El paquete de petición ARP dice "Si tu dirección IP coincide con esta dirección IP destino, por favor dime tu dirección Ethernet". Un paquete de petición ARP es algo similar a esto:

```
--------------------------------------------
|Dirección IP remitente 223.1.2.1          |
|Dirección Enet remitente 08-00-39-00-2F-C3|
--------------------------------------------
|Dirección IP destinatario   223.1.2.2     |
|Dirección Enet destinatario <blanco>      |
--------------------------------------------
```

TABLA 2. Ejemplo de petición ARP

Cada módulo ARP examina la dirección IP y si la dirección IP destino coincide con la propia dirección IP, envía una respuesta directamente a la dirección Ethernet origen. El paquete respuesta ARP dice "Si, esta dirección IP es mía, déjame darte mi dirección Ethernet". Un paquete respuesta ARP tiene el contenido del campo origen/destino intercambiado comparándolo con el paquete de petición. Tiene un aspecto como este:

```
--------------------------------------------
|Dirección IP remitente  223.1.2.2         |
|Dirección Enet remitente 08-00-28-00-38-A9|
--------------------------------------------
|Dirección IP destinatario  223.1.2.1      |
|Dirección Enet dest.  08-00-39-00-2F-C3   |
--------------------------------------------
```

TABLA 3. Ejemplo de respuesta ARP

La respuesta es recibida por el computador remitente original. El driver Ethernet mira el campo de tipo de la trama Ethernet y después pasa el paquete ARP al módulo ARP. El módulo ARP examina el paquete ARP y añade las direcciones IP y Ethernet del remitente a su tabla ARP.

La tabla actualizada ahora tiene un aspecto como este:

```
----------------------------------
|dirección IP  dirección Ethernet|
----------------------------------
|223.1.2.1      08-00-39-00-2F-C3|
|223.1.2.2      08-00-28-00-38-A9|
|223.1.2.3      08-00-5A-21-A7-22|
|223.1.2.4      08-00-10-99-AC-54|
----------------------------------
```

TABLA 4. Tabla ARP después de la respuesta

4.4 Continuación del escenario

La nueva traducción ha sido ahora instalada automáticamente en la

tabla, tan solo milisegundos después de que fuera necesaria. Si usted recuerda el paso 2 anterior, el paquete IP había sido puesto en cola de espera. Después, se realiza la traducción de la dirección IP a la dirección Ethernet mirando en la tabla ARP y después la trama Ethernet se transmite a la Ethernet. Por lo tanto, para los nuevos pasos 3,4 y 5 el escenario para el computador emisor es:

1. Un paquete de petición ARP con una dirección Ethernet broadcast se ha enviado a la red hacia cada computador.

2. El paquete IP de salida se pone en una cola de espera.

3. La respuesta ARP llega con la traducción IP a Ethernet para la tabla ARP.

4. Para el paquete IP en la cola, la tabla ARP se usa para traducir la dirección IP a la dirección Ethernet.

5. La trama Ethernet es transmitida hacia la Ethernet.

En resumen, cuando no se encuentra la traducción en la tabla ARP, un paquete IP se pone en cola de espera. Los datos de traducción se rellenan rápidamente mediante una petición/respuesta ARP y el paquete IP que estaba en la cola es transmitido.

Cada computador tiene una tabla ARP diferente para cada interfase Ethernet. Si el computador destino no existe, no hay respuesta ARP ni entrada en la tabla ARP. IP descartará los paquetes de salida dirigidos a esa dirección. La capa superior de protocolos no puede decir cual es la diferencia entre una Ethernet sin conexión y la ausencia de un computador con la dirección IP destino.

Alguna implementaciones de IP y ARP no ponen en cola el paquete IP mientras se espera a la respuesta ARP. En lugar de esto, el paquete IP se descarta y la recuperación de la pérdida del paquete IP se deja al módulo TCP o a la aplicación de red UDP. Esta recuperación se realiza mediante time-out (tiempo de espera agotado) y retransmisión. El mensaje retransmitido se envía con éxito a la red debido a que la primera copia del mensaje causó que se rellenase la tabla ARP.

El módulo IP es primordial para la tecnología internet y la esencia de IP es su tabla de enrutamiento. IP usa esta tabla en memoria para tomar todas las decisiones sobre enrutar un paquete IP. El contenido de la tabla de enrutamiento está definido por el administrador de red. Los errores bloquean la comunicación.

Entender como se usa una tabla de enrutamiento es entender el internetworking. Este conocimiento es necesario para el éxito de la

administración y el mantenimiento de una red IP.

La tabla de enrutamiento se entiende mejor echando un primer vistazo al enrutamiento, en lugar de aprender acerca de las direcciones IP, y después observando los detalles.

5.1 Enrutamiento directo

La figura siguiente es una pequeña internet con tres computadores: A, B y C. Cada computador tiene la misma pila de protocolos TCP/IP de la Figura 1. Cada interfase Ethernet de un computador tiene su

propia dirección Ethernet. Cada computador tiene una dirección IP asignada al interfase IP por el administrador de red, el cual también ha asignado un número de red IP a la Ethernet.

```
A      B      C
|      |      |
--o------o------o--
Ethernet 1
Red IP "Desarrollo"
```

Figura 6. Una red IP

Cuando A envía un paquete IP a B, la cabecera IP contiene la dirección IP de A como la dirección origen IP, y la cabecera Ethernet contiene la dirección Ethernet de A como la dirección Ethernet origen. Igualmente, la cabecera IP contiene la dirección IP de B como la dirección destino IP, y la cabecera Ethernet contiene la dirección Ethernet de B como la dirección Ethernet destino.

dirección	fuente	destino
Cabecera IP	A	B
Cabecera Ethernet	A	B

TABLA 5. Direcciones en un marco Ethernet para un paquete IP desde A hacia B

En este caso simple, la información IP es pasada por alto, ya que IP añade poco al servicio ofrecido por Ethernet. Sin embargo, IP añade coste: el proceso extra de CPU y el ancho de banda para generar, transmitir y parsear la cabecera IP.

Cuando el módulo IP de B recibe el paquete IP desde A compara la dirección destino IP con la propia, buscando coincidencias, después

pasa el datagrama al protocolo de nivel superior.

Esta comunicación entre A y B usa enrutamiento directo.

5.2 Enrutamiento indirecto

La figura siguiente muestra una visión más realista de una internet. Está compuesta por tres Ethernet y tres redes IP conectadas mediante un router IP llamado computador D. Cada red IP tiene cuatro computadores; cada computador tiene su propia dirección IP y Ethernet.

```
A      B      C      ----D----      E      F      G
|      |      |      |   |   |      |      |      |
--o------o------o------o-  |  -o------o------o------o--
Ethernet 1                 |  Ethernet 2
Red IP "Desarrollo"        |  Red IP "Contabilidad"
                           |
                           |
                           |     H      I      J
                           |     |      |      |
                         --o-----o------o------o--
                           Ethernet 3
                           Red IP "Taller"
```

Figura 7. Tres redes IP; una internet

Excepto para el computador D, cada computador tiene una pila TCP/IP como la de la Figura 1. El computador D es el router IP; está conectado a las tres redes y por consiguiente tiene tres direcciones IP y tres direcciones Ethernet. El computador D tiene una pila de protocolos TCP/IP similar a la Figura 3, excepto en que tiene tres módulos ARP y tres drivers Ethernet en lugar de dos. Por favor, observe que el computador D tiene sólo un módulo IP.

El administrador de red ha asignado un número único, llamado un número IP de red, a cada una de las Ethernet. Los números IP de red no se muestran en este diagrama, sólo los nombres de la red.

Cuando el computador A envía un paquete IP al computador B, el proceso es idéntico al ejemplo anterior de una red simple. Cualquier comunicación entre computadores localizada en una red IP sencilla concuerda con el ejemplo de enrutamiento directo explicado anteriormente.

Cuando el computador D y A se comunican, es comunicación directa.
Cuando el computador D y E se comunican, es comunicación directa.
Cuando el computador D y H se comunican, es comunicación directa.

Esto es debido a que cada una de estas parejas de computadores están en la misma red IP.

En cualquier caso, cuando el computador A se comunica con un computador en el lado más alejado del router IP, la comunicación ya no es directa. A debe usar a D para reenviar el paquete IP a la próxima red IP. Esta comunicación se llama indirecta.

Este enrutamiento de los paquetes IP se hace por los módulos IP y ocurre de forma transparente para TCP, UDP y las aplicaciones de red.

Si A envía un paquete IP a E, la dirección origen IP y la dirección origen Ethernet son las de A. La dirección IP destino es la de E, pero como el módulo IP de A envía el paquete IP a D para que lo reenvíe, la dirección Ethernet destino es la de D.

dirección	fuente	destino
cabecera IP	A	E
cabecera Ethernet	A	D

TABLA 6. Direcciones en una trama Ethernet para un paquete IP desde A hacia E (antes de pasar por D)

El módulo IP de D recibe el paquete IP y examinando la dirección destino IP dice "Esta no es mi dirección IP" y envía el paquete directamente hacia E.

dirección	fuente	destino
cabecera IP	A	E
cabecera Ethernet	D	E

TABLA 7. Direcciones en una trama Ethernet para un paquete IP

desde A hacia E (tras pasar por D)

En resumen, para la comunicación directa, tanto la dirección IP origen como la dirección Ethernet origen son del remitente, y la dirección IP y Ethernet destino son del destinatario. Para la comunicación indirecta la dirección IP y la Ethernet no se emparejan de esta forma.

Esta internet de ejemplo es una muy simple. Las redes reales son usualmente más complicadas por varios factores, teniendo múltiples routers IP y muchos tipos de redes físicas. Esta internet del ejemplo

podría surgir debido a que el administrador de red quisiera dividir una Ethernet grande para localizar el tráfico broadcast Ethernet.

5.3 Tablas de enrutamiento del módulo IP

Este vistazo al enrutamiento ha mostrado qué ocurre, pero no como ocurre. Ahora, examinemos las reglas o algoritmos usados por el módulo IP.

Para un paquete IP de salida, entrando desde una capa superior, IP debe decidir tanto enviar el paquete IP directa o indirectamente como elegir un interfase de red inferior. Estas elecciones se realizan consultando la tabla de enrutamiento.

Para un paquete IP de entrada, entrando desde un interfase inferior, IP debe decidir tanto reenviar el paquete IP o pasarlo hacia una capa superior. Si el paquete IP va a ser reenviado, se trata como un paquete IP de salida.

Cuando un paquete IP de entrada llega nunca es reenviado de nuevo a través del mismo interfase por el que ha llegado.

Estas decisiones se hacen antes de que el paquete IP se pase hacia el interfase inferior y antes de que se consulte la tabla ARP.

5.4 Dirección IP

El administrador de red asigna una dirección IP a los computadores de acuerdo con la red IP a la cual están conectados. Una parte de los cuatro bytes de la dirección IP es la dirección de red, la otra parte es el número IP del computador (o número de host). Para el computador en la tabla 1, con la dirección IP 223.1.2.1, el número de red es 223.1.2 y el número de host es 1.

La porción de la dirección que se usa para número de red y para número de host se define mediante los bits superiores en una dirección de cuatro bytes. Todos los ejemplos de direcciones IP en este tutorial son de clase C, lo que significa que los tres bits superiores de la dirección (110) indican que el número de red será de 21 bits y el número de host de ocho bits. Esto permite 2.097.152 redes de clase C con 254 computadores en cada red.

El espacio de direcciones IP lo administra el NIC (Network Information Center). Todas las internets que están conectadas a la misma Internet de alcance mundial deben usar número de red asignados por el NIC. Si usted está montando su propia internet y no está pensando en conectarla a la Internet, aún así debería obtener sus números de red del NIC. Si usted escoge su propio número, podría

correr el riesgo de producirse confusiones y caos en el caso de que su internet esté conectada a otra internet.

5.5 Nombres

La gente se refiere a los computadores mediante nombres, no mediante números. Un computador llamado alfa puede tener la dirección IP 223.1.2.1. Para redes pequeñas, estos datos de traducción de nombre a dirección suelen estar en cada computador en el archivo "hosts". Para redes mayores, este archivo de datos de traducción se guarda en un servidor y se accede desde cualquier punto de la red cuando se necesita. Algunas líneas de este archivo podrían ser como sigue:

```
223.1.2.1     alfa
223.1.2.2     beta
223.1.2.3     gamma
223.1.2.4     delta
223.1.3.2     epsilon
223.1.4.2     iota
```

La dirección IP está en la primera columna y el nombre de computador está en la segunda columna.

En muchos casos, usted puede instalar archivos "hosts" idénticos en todos los computadores. Usted puede reparar en que "delta" tiene sólo una entrada en este archivo incluso aunque tenga tres direcciones IP. "Delta" puede ser alcanzado con cualquiera de estas direcciones IP; no importa cual de ellas use. Cuando delta recibe un paquete IP y mira la dirección destino, reconoce cualquiera de sus propias direcciones IP.

A las redes IP también se les dan nombres. Si usted tiene tres redes IP, su archivo "redes" para documentar estos nombre puede ser algo como esto:

```
223.1.2     desarrollo
223.1.3     contabilidad
223.1.4     taller
```

El número de red IP está en la primera columna y su nombre está en la segunda columna.

De este ejemplo puede ver que "alfa" es el computador número 1 en la red de "desarrollo", beta es el computador número 2 en la red de "desarrollo" y así sucesivamente.

El siguiente archivo "hosts" es adecuado para los usuarios, pero el administrador de red probablemente cambiará la línea de "delta" con:


```
223.1.2.4     desnetrouter    delta
223.1.3.1     connetrouter
223.1.4.1     talnetrouter
```

Estas tres nuevas líneas para el archivo "hosts" dan a cada una de las direcciones IP de "delta" un nombre significativo. De hecho, la primera IP listada tiene dos nombres, "delta" y "desnetrouter" son

sinónimos. En la práctica "delta" es el nombre de propósito general para el computador y los otros tres nombres sólo se usan cuando se administra la tabla de enrutamiento IP.

Estos archivos son usados por las órdenes de administración de red y las aplicaciones de red para ofrecer nombres significativos. No se requieren para operar en una internet, pero nos lo hacen más fácil.

5.6 Tabla de enrutamiento IP

¿Cómo sabe IP qué interfase inferior de red usar cuando se envía un paquete? IP busca en la tabla de enrutamiento usando una búsqueda de clave del número de red IP extraído de la dirección IP destino.

La tabla de enrutamiento contiene una línea para cada ruta. Las columnas principales en la tabla de enrutamiento son: número de red IP, indicador de directo/indirecto, dirección IP del router y número de interfase. Esta tabla es usada por IP en cada paquete de salida.

En muchos computadores, la tabla de enrutamiento puede ser modificada con la orden "route". El contenido de la tabla de enrutamiento está definido por el administrador de red, ya que el administrador de red asigna las direcciones IP a los computadores.

5.7 Detalles del enrutamiento directo

Para explicar como se usa, visitemos en detalle las situaciones de enrutamiento que hemos revisado anteriormente.

```
                        ---------         ---------
                        | alfa  |         | beta  |
                        |    1  |         |  1    |
                        ---------         ---------
                             |               |
                       --------o---------------o-
                        Ethernet 1
                        red IP "desarrollo"
```

Figura 8. Vista de una red IP

La tabla de enrutamiento de "alfa" será como sigue:

red	señalador directo/indirecto	router	número de interfase
desarrollo	directo	<blanco>	1

TABLA 8. Ejemplo de tabla de enrutamiento simple

Esta vista puede ser vista en algunos sistemas UNIX con la orden "netstat -r". En esta red simple, todos los computadores tienen tablas de enrutamiento idénticas.

Para discutirla, se imprime de nuevo la tabla sin el número de red traducido a su nombre de red.

red	señalador directo/indirecto	router	número de interfase
223.1.2	directo	<blanco>	1

TABLA 9. Ejemplo de tabla de enrutamiento simple con números

5.8 Escenario directo

"Alfa" está enviando un paquete IP a "beta". El paquete IP está en el módulo IP de "alfa" y la dirección IP destino es "beta" o 223.1.2.2. IP extrae la porción de red de esta dirección IP y busca una entrada igual en la primera columna de la tabla. En esta red, se encuentra una concordancia en la primera entrada.

La otra información en esta entrada indica que en esta red se puede acceder a los computadores directamente a través del interfase 1. Se usa la tabla de traducción ARP para traducir la dirección IP de "beta" y después se envía la trama Ethernet directamente a "beta" vía el interfase número 1.

Si una aplicación intenta enviar datos a una dirección IP que no está en la red de "desarrollo", IP no será capaz de encontrar una entrada en la tabla de enrutamiento y descartará el paquete IP. Algunos computadores envían un mensaje de error de "red no alcanzable".

5.9 Detalles del enrutamiento indirecto

Ahora, echemos una mirada más cercana al escenario de enrutamiento un poco más complicado que habíamos examinado anteriormente.


```
         ---------          ---------          ---------
         | alfa  |          | delta |          |epsilon|
         |    1  |          |1  2  3|          |   1   |
         ---------          ---------          ---------
              |              |  |  |               |
     --------o---------------o- | -o---------------o--------
     Ethernet 1                |  Ethernet 2
     Red IP "Desarrollo"       |  Red IP "Contabilidad"
                               |
                               |     --------
                               |     | iota |
                               |     |  1   |
                               |     --------
                               |        |
                             --o--------o--------
                                 Ethernet 3
                                 Red IP "Taller"
```

Figura 9. Vista cercana de tres redes IP

La tabla de enrutamiento de "alfa" será como esta:

red	señalador	directo/indirecto	router	número de interfase
desarrollo	directo	<blanco>	1	
contabilidad	indirecto	desnetrouter	1	
taller	indirecto	desnetrouter	1	

TABLA 10. Tabla de enrutamiento de "alfa"

Para su discusión, la tabla se muestra de nuevo usando números en lugar de nombres.

red	señalador directo/indirecto	router	número de interfase
223.1.2	directo	<blanco>	1
223.1.3	indirecto	223.1.2.4	1
223.1.4	indirecto	223.1.2.4	1

TABLA 11. Tabla de enrutamiento de "alfa" con números

El router en la tabla de enrutamiento de "alfa" es la dirección IP de la conexión de "delta" a la red de "desarrollo".

5.10 Escenario indirecto

"Alfa" está enviando un paquete IP a "epsilon". El paquete IP está en el módulo IP de "alfa" y la dirección IP destino es la de "epsilon" (223.1.3.2). IP extrae la porción de red de esta dirección IP (223.1.3) y busca en la primera columna de la tabla una correspondencia. La encuentra en la segunda entrada.

Esta entrada indica que los computadores en la red 223.1.3 pueden ser alcanzados a través del router IP "desnetrouter". El módulo IP de "alfa" hace una traducción ARP para la dirección IP de "desnetrouter" y envía el paquete IP directamente a "desnetrouter" a través del interfase 1 de "alfa". El paquete IP todavía contiene la dirección IP destino de "epsilon".

El paquete IP llega al interfase de la red de "desarrollo" de "delta" y se pasa al módulo IP. La dirección IP destino se examina y como no concuerda con ninguna de las direcciones IP propias de "delta", éste decide reenviar el paquete IP.

El módulo IP de "delta" extrae la porción de red de la dirección IP destino (223.1.3) y busca un campo con ese número en su tabla de enrutamiento. La tabla de enrutamiento de "delta" sería como sigue:

red	señalador directo/indirecto	router	número de interfase
desarrollo	directo	<blanco>	1
taller	directo	<blanco>	2
contabilidad	directo	<blanco>	3

TABLA 12. Tabla de enrutamiento de "delta"

A continuación se muestra nuevamente la tabla de delta, sin la traducción de nombres.

red	señalador directo/indirecto	router	número de interfase
223.1.2	directo	<blanco>	1
223.1.4	directo	<blanco>	2
223.1.3	directo	<blanco>	3

TABLA 13. Tabla de enrutamiento de "delta" con números

Se encuentra una concordancia en la segunda entrada. IP después envía el paquete IP directamente a "epsilon" a través del interfase número

3. El paquete IP contiene la dirección IP de "epsilon" y la dirección Ethernet de "epsilon".

El paquete IP llega a "epsilon" y se pasa al módulo IP de "epsilon". La dirección IP de destino se examina y se encuentra que coincide con la IP de "epsilon", por lo cual el paquete se pasa a la capa superior de protocolo.

5.11 Resumen de enrutamiento

Cuando un paquete IP viaja a través de una internet larga, puede atravesar muchos routers IP antes de llegar a su destino. El camino que toma no se determina por una fuente central, ya que es el resultado de consultar cada una de las tablas de enrutamiento usadas en el viaje. Cada computador define sólo el siguiente salto en el viaje y se confía en ese computador para enviar el paquete IP de esta forma.

5.12 Administrando las rutas

Mantener las tablas de enrutamiento con información correcta en una internet grande es una tarea difícil; la configuración de red es modificada constantemente por los administradores de red para adecuarse a las necesidades. Los errores en las tablas de enrutamiento pueden bloquear la comunicación de forma que sea extremadamente tedioso hacer un diagnóstico.

Mantener una configuración de red simple nos lleva por un largo camino hacia conseguir una internet confiable. Por ejemplo, él método más directo para asignar redes IP a Ethernet es asignar un número de red IP simple para cada Ethernet.

También puede conseguir ayuda de ciertos protocolos y aplicaciones de red. ICMP (Internet Control Message Protocol - Protocolo de Mensajes de Control de Internet) puede avisar de algunos problemas de enrutamiento. Para redes pequeñas la tabla de enrutamiento se llena manualmente en cada computador por el administrador de red. Para redes mayores, el administrador de red automatiza esta operación manual con un protocolo de enrutamiento para distribuir las rutas por la red.

Cuando un computador se mueve de una red IP a otra, su dirección IP debe cambiar. Cuando un computador se elimina de una red IP, su antigua dirección será inválida. Estos cambios necesitan frecuentes actualizaciones del archivo "hosts". Este archivo de texto puede resultar difícil de mantener incluso para redes de tamaño medio. El DNS (Domain Name System - Sistema de Nombres de Dominio) ayuda a resolver estos problemas.

6. UDP (User Datagram Protocol -Protocolo de Datagrama de Usuario)

UDP es uno de los dos principales protocolos que residen por encima de IP. Ofrece servicio a las aplicaciones de red de usuario. Algunos ejemplos de aplicaciones de red que usan UDP son: NFS (Network File

System - Sistema de Archivos de Red) y SNMP (Simple Network Management Protocol - Protocolo de Administración de Red Simple). El servicio es un poco más que un interfase a IP.

UDP es un servicio de entrega de datagramas no orientado a conexión, lo cual no garantiza la entrega. UDP no mantiene una conexión de extremo a extremo con el módulo UDP remoto; simplemente envía el datagrama a la red y acepta datagramas de entrada de la red.

UDP añade dos valores a los servicios provistos por IP. Uno de ellos es la multiplexación de la información entre aplicaciones basándose en el número de puerto. El otro es una suma de comprobación (checksum) para comprobar la integridad de los datos.

6.1 Puertos

¿Cómo un cliente en un computador alcanza el servidor en otro?

El camino de la comunicación entre una aplicación y UDP se hace a través de los puertos UDP. Estos puertos están numerados, empezando por cero. Una aplicación que ofrece servicios (el servidor) espera mensajes que vengan dirigidos hacia un puerto específico dedicado para ese servicio. El servidor espera pacientemente a cualquier cliente que demande el servicio.

Por ejemplo, el servidor SNMP, llamado agente SNMP, siempre espera en el puerto 161. Sólo puede haber un agente SNMP por computador debido a que sólo hay un puerto 161. Este número de puerto es bien conocido; es un número fijo asignado para internet. Si un cliente SNMP quiere servicio, envía su petición al puerto UDP 161 del computador destino.

Cuando una aplicación envía datos a través de UDP llega al destino remoto como una unidad simple. Por ejemplo, si una aplicación escribe cinco veces al puerto UDP, la aplicación remota leerá cinco veces del puerto UDP. Del mismo modo, el tamaño de cada escritura coincide con el tamaño de cada lectura.

UDP conserva los límites del mensaje definidos por la aplicación. Nunca une dos mensajes de aplicación juntos o divide un mensaje de aplicación en dos partes.

6.2 Checksum - Suma de comprobación

Un paquete IP entrante con un campo de tipo en la cabecera IP indicando UDP se pasa al módulo UDP a través de IP. Cuando el módulo

UDP recibe el datagrama UDP desde IP examina la suma de comprobación UDP. Si esta suma es cero, ésto significa que no fue calculada por la aplicación y puede ser ignorada. De este modo, el módulo UDP del computador remitente puede o no generar sumas de comprobación. Si la red entre dos módulos UDP es sólo Ethernet, puede que no sea necesario hacer esta suma. En cualquier caso, es recomendable habilitar siempre su generación ya que en algún momento futuro un cambio en la tabla de enrutamiento pude hacer que los datos pueden ser enviados a través de un medio menos confiable.

Si la suma de comprobación es válida (o cero) el número de puerto destinatario se examina y si la aplicación está limitada a este puerto, un mensaje de aplicación, un mensaje de aplicación se pone en cola de espera para ser leído por la aplicación. De otro modo, el datagrama UDP se descarta. Si el datagrama UDP entrante llega más rápido de lo que la aplicación pueda leerlo y si la cola está llena

al máximo, el datagrama UDP es descartado por UDP. UDP continuará descartando datagramas hasta que haya espacio en la cola.

7. TCP (Transmission Control Protocol - Protocolo de Control de la Transmisión)

   TCP ofrece un servicio diferente que UDP. TCP ofrece un flujo de bytes orientado a conexión, en lugar de un servicio de entrega de datagramas no orientado a conexión. TCP garantiza la entrega, mientras que UDP no lo hace.

   TCP es usado por las aplicaciones de red que quieren garantía de entrega y no pueden ser molestados haciendo time-outs (tiempo de espera agotado) y retransmisiones. Las dos aplicaciones de red más típicas que usan TCP son FTP (File Transfer Protocol - Protocolo de Transferencia de Ficheros) y TELNET. Otras aplicaciones de red populares incluyen el sistema X-Window, rcp (copia remota) y la serie de órdenes r. La mayor capacidad de TCP no es gratis: requiere más CPU y ancho de banda de red. Las interioridades del módulo TCP son mucho más complicadas que las de un módulo UDP.

   De forma similar a UDP, las aplicaciones conectan a los puertos TCP. Los números de puertos bien definidos se dedican a aplicaciones específicas. Por ejemplo, el servidor de TELNET usa el número de puerto 23. El cliente TELNET puede encontrar el servidor sencillamente conectándose al puerto TCP 23 del computador especificado.

   Cuando la aplicación empieza a usar TCP, el módulo TCP del computador del cliente y el módulo TCP del computador servidor empiezan a comunicarse entre si. Estos dos módulos TCP finales contienen información de estado que define el circuito virtual. Este circuito

   virtual consume recursos en ambos puntos finales TCP. El circuito virtual es full-duplex (bidireccional); los datos pueden ir en ambos sentidos simultáneamente. La aplicación escribe datos en el puerto TCP, los datos atraviesan la red y son leídos por la aplicación en el destino remoto.

   TCP empaqueta el flujo de bytes como quiere; no conserva los límites del mensaje entre escrituras. Por ejemplo, si una aplicación hace cinco escrituras al puerto TCP, la aplicación remota puede hacer diez lecturas para recuperar todos los datos. O incluso leer todos los datos de una sola vez. No hay relación entre el número y el tamaño de las escrituras en un extremo y el tamaño de las lecturas en el otro extremo.

   TCP es un protocolo de ventana deslizante con time-out (agotamiento del tiempo de espera) y retransmisión. Los datos salientes deben ser reconocidos por el extremo remoto TCP. Los reconocimientos (acknowledgement - ACK) pueden ser enviados junto con mensajes de datos. Ambos extremos pueden controlar el flujo del extremo remoto, lo cual previene el desbordamiento de los buffers (memorias temporales intermedias).

   Como todos los protocolos de ventana deslizante, el protocolo tiene tamaño de ventana. El tamaño de la ventana determina la cantidad de datos que pueden ser transmitidos antes de que se requiera un reconocimiento. Para TCP, esta cantidad no es un número de segmentos TCP, sino un número de bytes.

8. Aplicaciones de red

¿Por qué existen tanto TCP como UDP, en lugar de sólo uno o el otro?

Proveen diferentes servicios. Muchas aplicaciones están implementadas para usar solo uno u otro. Usted, el programador, elije el protocolo que mejor satisface sus necesidades. Si necesita un servicio de entrega confiable, TCP puede ser mejor. Si necesita un servicio de datagrama, UDP puede ser mejor. Si necesita eficiencia sobre circuitos de transporte extensos, TCP puede ser mejor. Si necesita eficiencia sobre redes rápidas con poca latencia, UDP puede ser mejor. Si sus necesidades no encajan dentro de estas categorías, entonces la "mejor" opción está poco clara. Sin embargo, las aplicaciones pueden disimular deficiencias en la elección. Por ejemplo si elige UDP y necesita confiabilidad, entonces la aplicación debe proveer confiabilidad. Si elige TCP y necesita un servicio orientado a grabación, entonces la aplicación debe insertar marcas en la trama de bytes para delimitar los registros.

¿Que aplicaciones de red están disponible?

Hay muchas para listar. El número está creciendo continuamente. Algunas de las aplicaciones han existido desde los comienzos de la tecnología internet: TELNET y FTP. Otros son relativamente nuevos: X-Windows y SNMP. Lo siguiente es una breve descripción de las aplicaciones mencionadas en este tutorial.

8.1 TELNET

TELNET provee una capacidad de ingreso remoto sobre TCP. La operación y apariencia es similar a un diálogo del teclado a través de una conexión telefónica. En la línea de órdenes el usuario escribe "telnet delta" y recibe un prompt de ingreso desde la computadora llamada "delta".

TELNET trabaja bien; es una antigua aplicación y ha extendido la interoperabilidad. Las implementaciones de TELNET usualmente trabajan entre diferentes sistemas operativos. Por ejemplo, un cliente TELNET puede estar en un VAX/VMS y el servidor en un UNIX System V.

8.2 FTP

File Transfer Protocol - Protocolo de Transferencia de Ficheros (FTP), antiguo como TELNET, también usa TCP y ha extendido la interoperabilidad. La operación y apariencia es como si usted TELNETeara a la computadora remota. Pero en lugar de escribir sus órdenes usuales, tiene que hacerlo con una pequeña lista de órdenes para listar directorios y lo que desee. Las órdenes FTP permiten copiar archivos entre computadoras.

8.3 rsh

Intérprete de órdenes remoto (rsh o remsh) es uno de una familia entera de órdenes de estilo UNIX remoto. La orden UNIX de copia, cp, se convierte en rcp. La orden UNIX "quien ingreso en", who, se convierte en rwho. La lista continúa y está referida a una colección como la serie de órdenes "r" o los órdenes "r*" (r estrella).

Las órdenes r* principalmente trabajan entre sistemas UNIX y son diseñados para interactuar entre hosts autenticados. Algunas precauciones son tomadas para seguridad, pero proveen un conveniente ambiente de usuario.

Para ejecutar la orden "cc file.c" en una computadora remota llamada delta, escriba "rsh delta cc file.c". Para copiar el fichero "file.c" a delta, escriba "rcp file.c delta:". Para ingresar a delta, escriba "rlogin delta", y si administró las computadoras en una cierta manera, no será desafiado con una clave.

8.4 NFS

Network File System - Sistema de Ficheros de Red, los primeros desarrollados por Sun Microsystems Inc, usa UDP y es excelente para montar sistemas de ficheros UNIX en múltiples computadoras. Una estación de trabajo bajo disco puede acceder al disco rígido del servidor como si el disco estuviese localizado en la estación de trabajo. Una copia simple de disco de una base de datos en un mainframe "alpha" puede también ser usada por el mainframe "beta" si el sistema de ficheros de la base de datos esta montada con NFS en "beta".

NFS agrega carga significativa a una red y tiene una pobre utilidad a través de conexiones lentas, pero los beneficios son grandes. El cliente NFS está implementado en el kernel, permitiendo todas las aplicaciones y órdenes para usar el disco NFS montado como si el disco fuese local.

8.5 SNMP

Simple Network Management Protocol - Protocolo de Administración de Red Simple (SNMP) usa UDP y esta diseñado para el uso de una estación de manejo de red central. Es un hecho bien conocido que si toma bastantes datos, un administrador de red puede detectar y diagnosticar problemas de red. La estación central usa SNMP para recolectar estos datos desde otras computadoras en la red. SNMP define el formato de los datos; le deja a la estación central o al administrador de red interpretar los datos.

8.6 X-Window

El sistema X-Window usa el protocolo X-Window en TCP para dibujar ventanas en la pantalla de una estación de trabajo. X-Window es mucho más que una utilidad para dibujar ventanas; es una filosofía entera para diseñar una interfaz de usuario.

9. Otra información

Mucha información sobre la tecnología de internet no fue incluida en este tutorial. Esta sección lista información que es considerada el próximo nivel de detalle para el lector que desea aprender más.

- órdenes de administración: arp, route y netstat
- ARP: entrada permanente, entrada pública, entrada de time-out, spoofing
- Tabla de encaminamiento IP: entrada de host, pasarela predeterminada, subredes
- IP: contador tiempo-de-vida, fragmentación, ICMP

- RIP, ciclos de encaminamiento
- Sistema de nombres de dominio

10. Referencias

[1] Comer, D., "Internetworking with TCP/IP Principles, Protocols, and Architecture", Prentice Hall, Englewood Cliffs, New Jersey, U.S.A., 1988.

[2] Feinler, E., et al, DDN Protocol Handbook, Volume 2 and 3, DDN Network Information Center, SRI International, 333 Ravenswood Avenue, Room EJ291, Menlow Park, California, U.S.A., 1985.

[3] Spider Systems, Ltd., "Packets and Protocols", Spider Systems Ltd., Stanwell Street, Edinburgh, U.K. EH6 5NG, 1990.

11. Relación con otros RFCs

Este RFC es un tutorial y no ACTUALIZA ni DEJA OBSOLETO ningún otro RFC.

12. Consideraciones de seguridad

Hay consideraciones de seguridad entre el conjunto de protocolos TCP/IP. Para muchas personas estas consideraciones son serios problemas, para otras no; depende de los requerimientos del usuario.

Este tutorial no discute estos asuntos, pero si quiere aprender más debe comenzar con el tema de ARP-spoofing, entonces vea la sección "Consideraciones de Seguridad" del RFC 1122 para tener más información.

13. Direcciones de los autores

Theodore John Socolofsky
Spider Systems Limited
Spider Park
Stanwell Street
Edinburgh EH6 5NG
United Kingdom

Phone:
from UK 031-554-9424
from USA 011-44-31-554-9424
Fax:
from UK 031-554-0649
from USA 011-44-31-554-0649

EMail: TEDS@SPIDER.CO.UK

Claudia Jeanne Kale
12 Gosford Place
Edinburgh EH6 4BJ
United Kingdom

Phone:
from UK 031-554-7432
from USA 011-44-31-554-7432

EMail: CLAUDIAK@SPIDER.CO.UK

Traducción al castellano: M.Angels Flores Guirola, A.J. Waisbrot (2002)